

RECEIVED
CENTRAL FAX CENTER PATENTS
DEC 20 2006 10/010,894
DOCKET 0960-021

IN THE CLAIMS

1.(Currently amended) A method of maintaining additional security for communications between an upstream server and at least two downstream client modems on a shared communication media through use of a dynamic key generated by the particular client modems, the method comprising:

A. the server receiving a scrambled upstream communication from a first client modem, wherein the upstream communication is a packet;

B. the server unscrambling a scrambled ~~portion of the upstream communication packet~~ containing a new key for the first client modem using a previous seed for the first client modem based on a previous key for the first client modem received in a previous upstream ~~communication packet~~ from the first client modem;

C. the server storing information sufficient to create a new seed for the first client modem based on the new key for the first client modem based on the unscrambled contents of the upstream ~~communication packet;~~

D. the server scrambling at least a portion of the next downstream communication to a second client modem with scrambling based on a seed for the second client modem based on a key for the second client modem, where in the key for the second client modem is unrelated to the key for the first client modem, wherein the downstream communication is a subpacket;

E. the server scrambling at least a portion of the next downstream ~~communication subpacket~~ to the first client modem with scrambling based on the new seed for the first client modem based on the new key for the first client modem;

F. the first client modem receiving the next downstream ~~communication subpacket~~ to scrambled for the first client modem;

G. the first client modem unscrambling the scrambled portion of the next downstream ~~communication subpacket~~ to scrambled for the first client modem with the new seed for the first client modem based on the new key for the first client modem;

H. the first client modem creating a next upstream ~~communication packet~~ containing a next key for the first client modem;

I. the first client modem storing information sufficient to create a next seed for the first client modem based on the next key for the first client modem; and

J. the first client modem scrambling at least a portion of the next upstream ~~communication packet~~ using the new seed for the first client modem based on the previously communicated new key for the first client modem.

2. (Original) The method of claim 1 wherein the new seed for the first client modem equals the new key for the first client modem.

3. (Currently amended) The method of claim 1 wherein the new key for the first client modem is a transmission check word used for the purpose of testing the accuracy of the upstream transmission, such that the new key for the first client modem is transmitted with the upstream ~~communication packet~~ without adding to the overhead.

4. (Original) The method of claim 1 wherein the new key for the first client

PATENTS
10/010,894
DOCKET 0960-021

modem is a random number generated by the first client modem and not a transmission check word.

5. (Currently amended) The method of claim 1 wherein the scrambled portion of the upstream ~~communication~~ packet includes a portion of the data packet header.

6. (Currently amended) The method of claim 5 wherein the scrambled portion of the upstream ~~communication~~ packet includes a field conveying the length of a variable length data packet.

7. (Currently amended) The method of claim 1 wherein first client modem unscrambles the scrambled portion of the next downstream ~~communication~~ subpacket to the first client modem with the new seed for the first client modem based on the new key for the first client modem only when a field in the next downstream communication lacks a signal to use a default seed based on a default key.

8. (Original) The method of claim 7 where the default key is based on the address of the first client modem.

9. (Currently amended) The method of claim 7 wherein the previous key for the first client modem received in a previous upstream ~~communication~~ packet from the first client modem was sent with scrambling based on the default key.

10. (Currently amended) The method of claim 1 further comprising the preliminary steps of exchanging ~~communications~~ upstream packets and downstream subpackets between the server and the first client modem, ~~a portion of~~ the preliminary communications scrambled with a default seed until the server has stored information sufficient to create an initial first client modem seed based on an initial first client modem key.

11. (Original) The method of claim 1 wherein a scrambled value is passed with one communication and the value is used to alter the DVB randomization of the next communication whereby the controlled variation in the DVB randomization provides a layer of security to protect the next communication from an eavesdropper as the eavesdropper would need the passed value in order to reverse the non-standard DVB randomization.

12. (Currently amended) The method of claim 1 wherein:
the server sent a multicast address key and a multicast address in the next downstream ~~communication~~ subpacket to the first client modem;
the server sent the same multicast address key and the same multicast address in the next downstream ~~communication~~ subpacket to the second client modem;
and further comprising the step of:
the server creating a multicast ~~communication~~ subpacket addressed to a multicast group comprising the first client modem and the second client modem;

PATENTS

10/010,894

DOCKET 0960-021

the server sending the multicast ~~communication~~ subpacket after scrambling a portion of the multicast communication with a seed based on the multicast address key.

13. (Currently amended) The method of claim 1 wherein the server scrambles ~~at least a portion of the next downstream communication~~ subpacket to the first client modem with a seed based on both:

the new key for the first client modem, and

an earlier key for the first client modem received before the new key for the first client modem.

14. (Currently amended) A method of maintaining additional security for communications between an upstream server and at least two downstream client modems on a shared communication media through use of a dynamic key generated by the server, the method comprising:

A. the server storing information sufficient to create a seed for the first client modem based on a key for the first client modem generated by the server, the key for the first client modem to be sent in a downstream communication to a first client modem, wherein the downstream communication is a subpacket;

B. a second client modem receiving a downstream ~~communication~~ subpacket from the server;

C. the second client modem unscrambling a scrambled portion of the downstream ~~communication~~ subpacket containing a new key for the second client modem using a seed for the second client modem based on a key for the second client modem received in a previous downstream ~~communication~~ subpacket from the server;

D. the second client modem storing information sufficient to create a new seed for the second client modem based on the new key for the second client modem received in the unscrambled contents of the downstream ~~communication~~ subpacket;

E. the second client modem scrambling ~~at least a portion of the next upstream communication~~ packet to the server with scrambling based on the new seed for the second client modem based on the new key for the second client modem, wherein the upstream communication is a packet;

F. the server receiving the next upstream ~~communication~~ packet from the second client modem;

G. the server unscrambling the scrambled portion of the next upstream ~~communication~~ packet from the second client modem with the new seed for the second client modem based on the new key for the second client modem;

H. the server creating a next downstream ~~communication~~ subpacket containing a next key for the second client modem;

I. the server storing information sufficient to create a next seed for the second client modem based on the next key for the second client modem without impacting the previously stored information sufficient to create the seed for the first client modem based on the first client modem key; and

J. the server scrambling at least a portion of the next downstream ~~communication~~ subpacket using the new seed for the second client modem based on the previously communicated new key for the second client modem.

PATENTS

10/010,894

DOCKET 0960-021

15. (Currently amended) A method of dynamic double scrambling of communications sent to and from a particular client modem; the method comprising the steps of:

A. a server identifies the existence and the address of first client modem on a shared transmission media;

B. the server creates and transmits a downstream communication addressed to the first client modem with a portion of the downstream communication scrambled twice based on two default scrambling seeds, the downstream communication containing a control field indicating that the default seeds were used, wherein the downstream communication is a subpacket;

C. the first client modem receives the downstream ~~communication~~ subpacket and recognizes that the default seeds were used;

D. the first client modem unscrambles the downstream ~~communication~~ subpacket using the default seeds;

E. the first client modem creates and transmits an upstream communication, before transmission the upstream communication scrambled twice with the two default seeds, the scrambled portion of the upstream communication containing a key created by the first client modem, wherein the upstream communication is a packet;

F. the server receives the upstream ~~communication~~ packet and the server unscrambles the scrambled ~~portion of the upstream communication~~ packet using the default seeds and stores the key created by the first client modem;

G. the server creates and transmits a downstream ~~communication~~ subpacket addressed to the first client modem with the control field indicating that the communication is scrambled using one default scrambling seed and one seed based on the key created by the first client modem, a portion of the downstream ~~communication~~ subpacket scrambled once with one default seed and once with one seed based on the key created by the first client modem, the scrambled ~~portion of the downstream communication~~ subpacket including a key created by the server for communication with the first client modem;

H. the first client modem receives the downstream ~~communication~~ subpacket and reads the control field;

I. the first client modem unscrambles the downstream ~~communication~~ subpacket using the one default seed and one seed based on the last transmitted key created by the first client modem;

J. the first client modem stores the key created by the server for communication with the first client modem;

K. the first client modem creates and transmits an upstream ~~communication~~ packet, before transmission ~~of a portion of the upstream communication~~ packet including the new key created by the first client modem is scrambled twice using the one seed based on the last transmitted key created by the first client modem and one seed based on the last transmitted server created key for communication with the first client modem;

L. the server receives the upstream ~~communication~~ packet, and unscrambles the upstream ~~communication~~ packet using one seed based on the previously stored key created by the first client modem and one seed based on the last transmitted server created key for communications with the first client modem;

M. the server stores the last transmitted key created by the first client modem;

PATENTS

10/010,894

DOCKET 0960-021

N. the server creates and transmits a downstream ~~communication~~ subpacket addressed to the first client modem with the control field indicating that the ~~communication~~ subpacket is scrambled using one seed based on the last transmitted key created by the first client modem and one seed based on the last transmitted server created key for communication with the first client modem; a portion of the downstream ~~communication~~ subpacket scrambled once with one seed based on the last transmitted key created by the first client modem and once with one seed based on the last transmitted server created key for communication with the first client, the scrambled portion of the downstream ~~communication~~ subpacket containing a new server created key for communication with the first client modem;

O. the first client modem receives the downstream ~~communication~~ subpacket and reads the control field;

P. the first client modem unscrambles the downstream ~~communication~~ subpacket using one seed based on the previously stored server created key for communication with the first client modem and one seed based on the last transmitted key created by the first client modem;

Q. the first client modem stores the last transmitted server created key for communication with the first client modem,

REPEAT steps K through Q;

UNTIL detecting a break in the communications between the first client modem and the server;

THEN GOTO Step B.

16. (Original) The method of claim 15 wherein the key created by the first client modem is a transmission check word.

17. (Original) The method of claim 15 wherein at least one of the default seeds is used solely for communications with the first client modem.

18. (Original) The method of claim 15 wherein at least one of the default seeds is derived from an address of the first client modem.

19. (Previously presented) A method of updating the keys used by a first device in a dynamic dual key scrambling system with the dual keys including a key created by a first device and a key created by a second device, the updating occurring when an incoming ~~communication~~ packet received at the first device contains a unique address for the first device and the incoming communication indicates the completion of the start up sequence to establish dynamic dual key scrambling between the first device and the second device, the method comprising:

A. Unscramble the scrambled portion of the incoming ~~communication~~ packet with a stored key created by the first device and a stored key created by the second device;

B. Store key created by the second device received in the scrambled portion of the incoming ~~communication~~ packet;

C. Create a new key created at the first device and include the new key in an the outgoing ~~communication~~ packet from the first device;

PATENTS

10/010,894

DOCKET 0960-021

D. Scramble portions of the outgoing ~~communication~~ packet including the new key created by the first device with the stored key from the first device and the stored key from the second device;

E. Store key created by the first device; and

F. Send outgoing ~~communication~~ packet.

20. (Original) The method of claim 19 wherein:

the stored key created by the first device used in the scrambling and unscrambling operations is the most recently stored key created by the first device, and

the stored key created by the second device used in the scrambling and unscrambling operations is the most recently stored key created by the second device.

21. (Original) The method of claim 19 wherein the stored key created by the first device used in the scrambling and unscrambling operations is not the most recently stored key created by the first device.

22. (Original) The method of claim 19 wherein the stored key created by the second device used in the scrambling and unscrambling operations is not the most recently stored key created by the second device.